LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

Orientation to Computing-I

L T P :2 0 0

Unit-5 (Security Essentials)

- Basic security threats (malwares, Phishing, Social engineering, Password cracking), Password management (Password complexity, Change default passwords)
- Open WiFi vs. secure WiFi, Multi Factor authentication, Admin vs. user vs. guest Account.

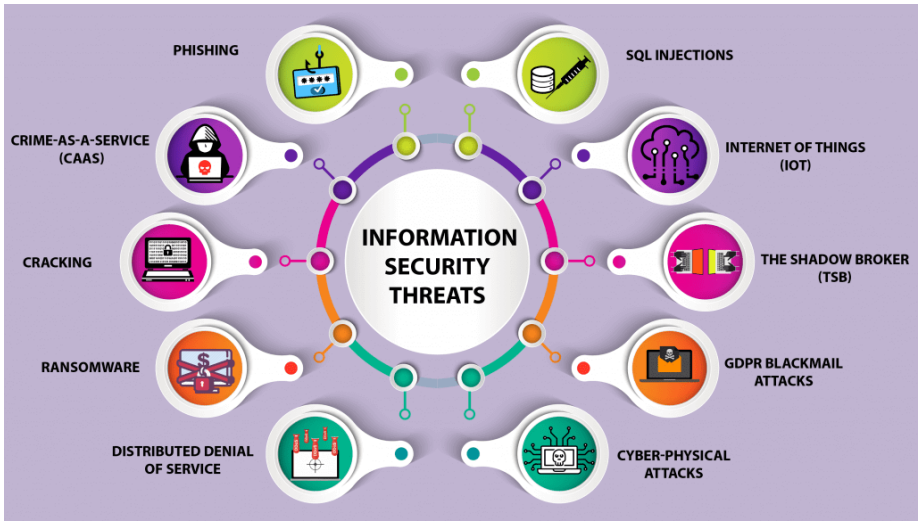
Unit-5 (Secure Web Browsing)

- Recognize a secure connection
- Recognize suspicious links, Update browsers and plugins
- Recognize untrusted source warnings, social media security (facebook, whatsapp, email).

Basic Security Threats

- Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

- Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

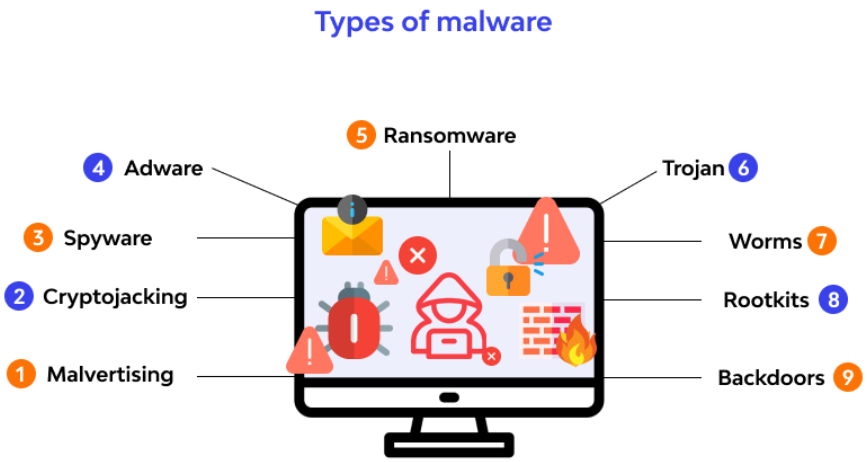


Types of Network Threats

- **Malware:** It is a malicious software mostly used by criminals to hold your system, steal your confidential data, or install damaging programs in your device without your knowledge. It spreads spyware, Trojans, and worms through pop-up ads, infected files, bogus websites, or e-mail messages.

- **Phishing:** This type of online fraud is designed to steal sensitive information, such as credit card numbers and passwords.
- Phishing attacks impersonate reputable banking institutions, websites, and personal contacts, which come in the form of immediate phishing e-mails or messages designed to look legitimate.
- Once you click the URL or reply to the messages, you are prompted to enter your financial details or use your credentials, which then sends your data to the malicious source.

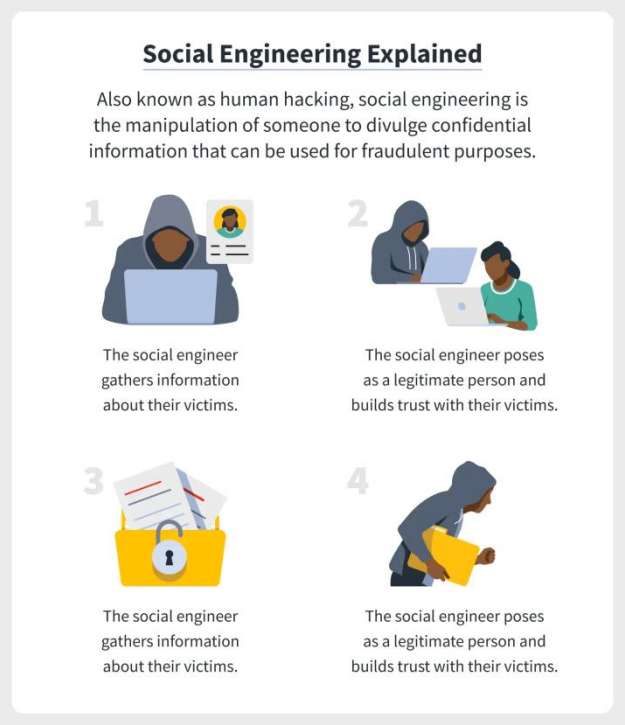
Malware and Phishing



30, 000 websites **are hacked every day**

Types of Network Threats

Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks or physical locations or for financial gain.

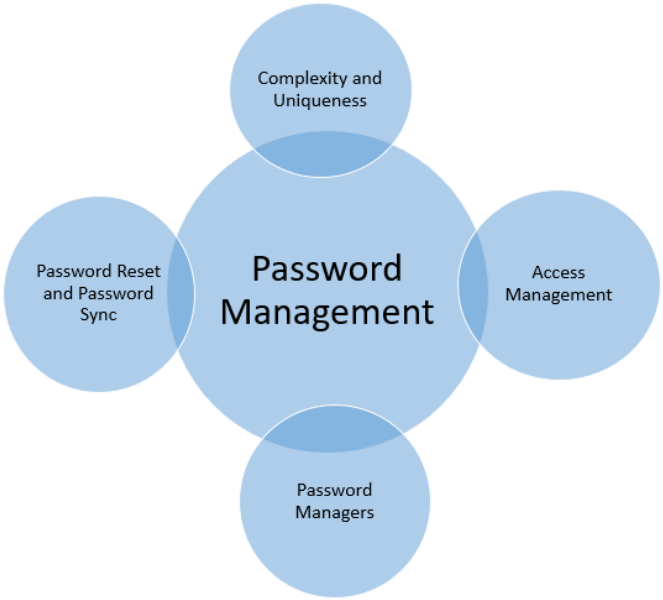


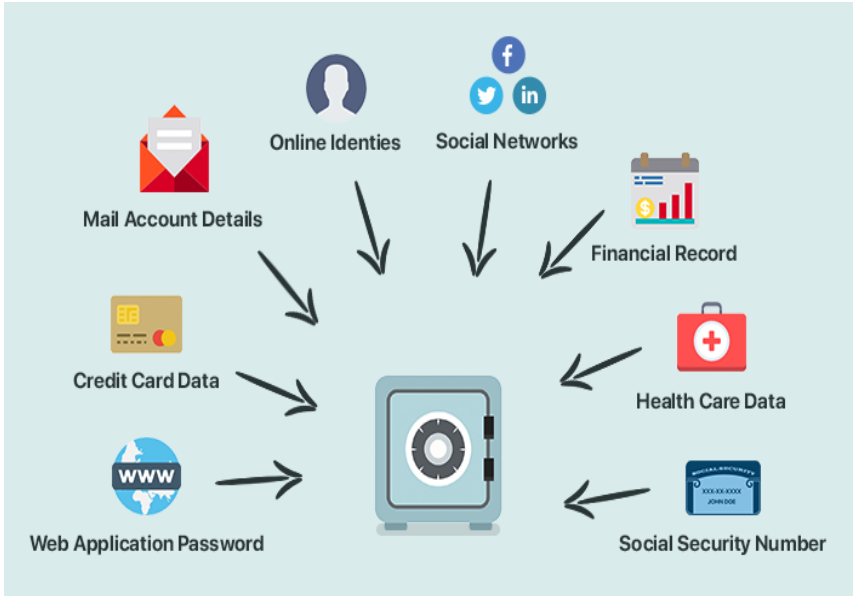
Types of Network Threats

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

Password Management

Password management is a system that allows users to store and access passwords securely. Password management is defined as a system that facilitates a simple, secure way to store passwords and access them quickly when required. Today, password management is a critical part of the IT policy of most organizations





Password complexity

Password complexity is a measure of how difficult a password is to guess in relation to any number of guessing or cracking methods.

In some cases, the term is also used to refer to requirements for password selection that are designed to increase password complexity in the interest of better security.

Password complexity is important because guessed passwords are a common avenue for attack, and thus, for data breaches.

When passwords can be guessed, individuals other than the owner of an account or resource are able to access that account or resource without permission.

Password complexity

- Password complexity guidelines often require users to create passwords according to particular rules—for example, the inclusion of a minimum number of special characters, numbers, lowercase and capital letters, and so on.
- These requirements, however, often have the effect of making passwords very difficult for users to remember and enter, which may have the paradoxical effect of reducing security as users seek to find ways to remember their passwords—for example, by writing them down or saving them in a convenient place.
- The US National Institute for Standards and Technology (NIST) has determined most password complexity guidelines to be outdated for this reason, and does not endorse most password complexity requirements.
- Instead, many experts now recommend the use of passphrases—very long passwords that are easier for users to remember, such as "YellowBoatCubumberNevadaIceCream" or "SevenSharkFitnessFandom" for example.

Default Passwords

What is Default Password?

- Factory default software configurations for embedded systems, devices, and appliances often include simple, publicly documented passwords. These systems usually do not provide a full operating system interface for user management, and the default passwords are typically identical (shared) among all systems from a vendor or within product lines. Default passwords are intended for initial testing, installation, and configuration operations, and many vendors recommend changing the default password before deploying the system in a production environment.

What is the Risk?

- Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet

Password Security

Open WiFi Vs Secure WiFI

Open WiFi

- An open wifi is just that: Open. There are no passwords.
- No barriers to entry. That means that you and anyone else can get on the network. Typically, on such networks you cannot see any other devices (if it is setup correctly), but you honestly don't know.
- It's best to assume that they can see everything that you do on the network and exercise caution. You don't know who is on that network with you. Don't go to banking or financial sites.
- Do not do company work on the wifi. Or access anything that you would not someone else to see.
- Assume that they can and be surprised if they can't. It works out better that way.

Open WiFi Vs Secure WiFI

Secure WiFi

- Secure Wi-Fi network refers to the use of passwords and secure encryption methods to send wireless data between a mobile device and the Internet connection point.

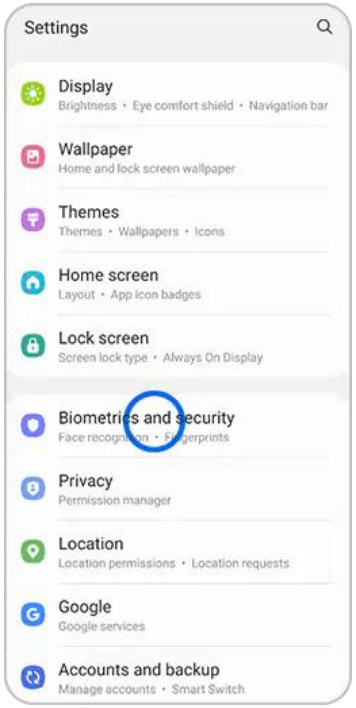
- There is more than one way to encrypt data. One method is Wi-Fi Protected Access-2 (WPA2).

- WPA-2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard.

Activity-1

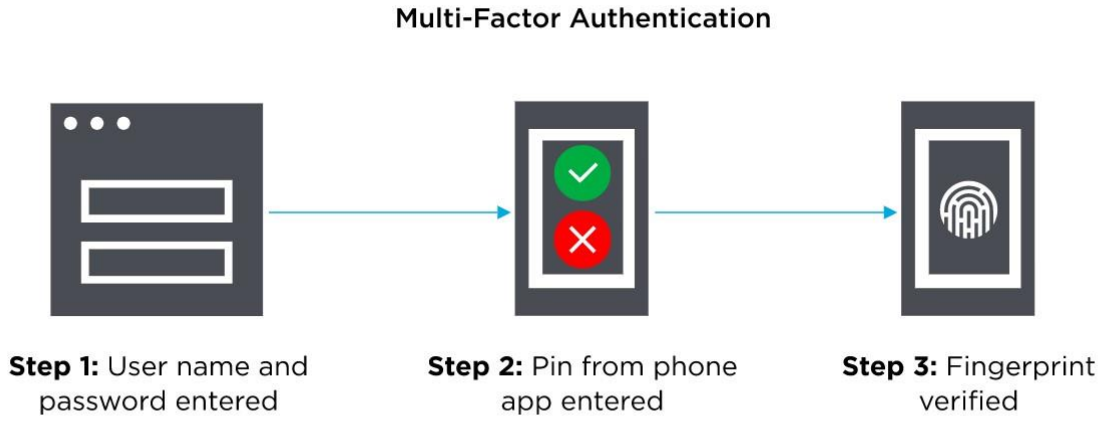
What is the secure Wifi feature & how do I enable or use it?

Our phone's Secure Wi-Fi feature lets you browse the internet safely, even when you're using unsecured, public Wi-Fi networks. It offers protection by encrypting internet traffic and blocking tracking apps



Multi Factor Authentication

- Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
- MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack..



Why is MFA Important?

- The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password.

- While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties.

- Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

How Does MFA work?

- MFA works by requiring additional verification information (factors). One of the most common MFA factors that users encounter are one-time passwords (OTP).

- OTPs are those 4-8 digit codes that you often receive via email, SMS or some sort of mobile app. With OTPs a new code is generated periodically or each time an authentication request is submitted.

- The code is generated based upon a seed value that is assigned to the user when they first register and some other factor which could simply be a counter that is incremented or a time value.

Three Main Types of MFA Authentication Methods

Most MFA authentication methodology is based on one of three types of additional information:

- Things you know (knowledge), such as a password or PIN
- Things you have (possession), such as a badge or smartphone
- Things you are (inherence), such as a biometric like fingerprints or voice recognition

Admin vs. user vs. guest Account.

- **Guests Accounts** are usually created when we want someone to have temporary access to your personal computer system. A guest account is a temporary account and the user is strictly not allowed to perform any changes to your PC settings or to access any of your personal files stored in the PC.
- Unlike the **Standard User** or **Administrator, Guest account** users cannot create a password, install a software on their PC, or can't even modify any of their PC settings. All a guest account user can do is to log on to your PC, browse and surf on the web and can shut down the PC. Guest Accounts have a limited set of permissions, but still, it is important to disable it when not being a user.

Admin vs. User vs. Guest Account

- The **Administrator account** is the first account that is created during the Windows installation. The Administrator account has full control of the files, directories, services, and other resources on the local computer. The Administrator account can create other local users, assign user rights, and assign permissions.
- A guest is an **anonymous user** account that provides access to a computer on a limited or temporary basis. Although some computer operating systems have guest accounts by default, most have to be set up manually by the computer's administrator.

Secure Web-Browsing

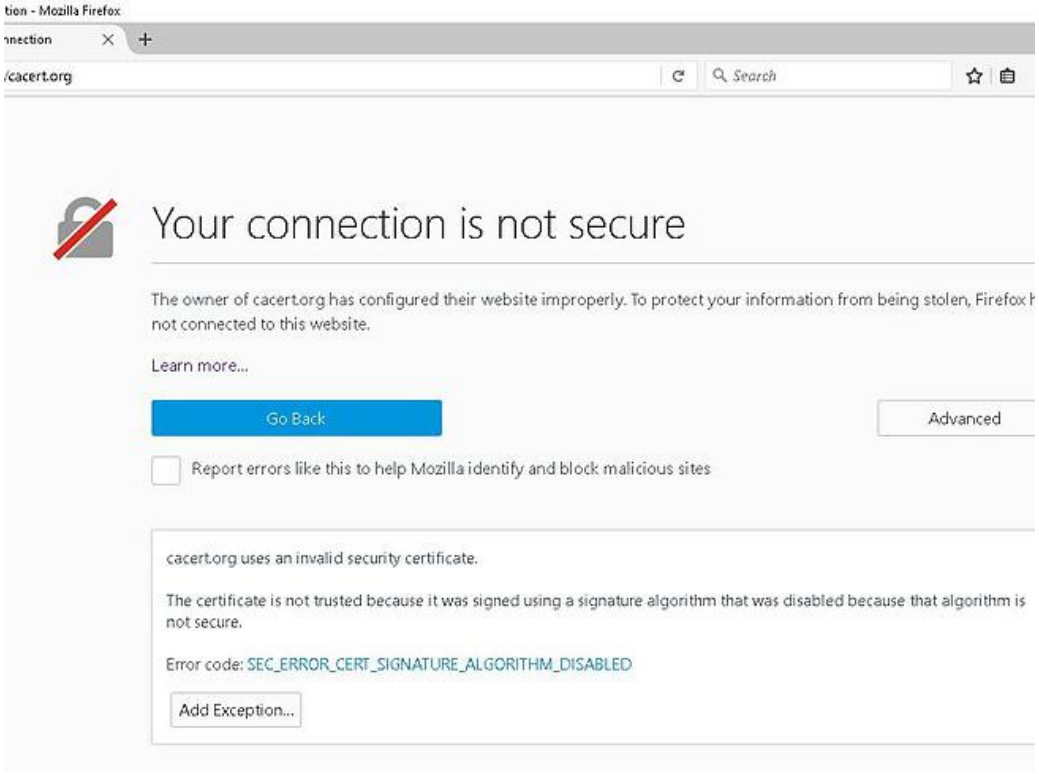
Secure web browsing involves the use of tools and techniques to protect users from cyberattacks, malware, or other cybersecurity vulnerabilities. Web browsers allow users to view sites on the internet by displaying images and text, executing code, rendering animations, and saving information.

Activity -4

How to secure your web browser (Google Chrome, Microsoft Edge, Firefox)

Secure Connection

Browsers will return a "connection not secure" error when they can't verify a website's SSL certificate. SSL is a secure data-encryption method that keeps transmitted data private and safe. If a browser detects a problem with a site's SSL certificate, it won't load that site because it might be unsafe. While all this can sound very alarming, it's likely that nothing is wrong.



Secure Connection

What Causes This Error?

- Many things can cause these errors warning about a connection that isn't secure, some of which are problems on the site's end.
- The website could have an expired SSL certificate, no SSL certificate, or one that wasn't set up correctly. Setting up SSL certificates is hard, especially if a site's administrators bought a higher-end certificate, and not everyone always gets it right. It's also possible that a trusted organization didn't issue the certificate.

Note: *To see if the site's SSL certificate is expired, select Not Secure on the top of the error window, and then Select Certificate. Check the Expires On date to see if the certificate is expired. If so, you can't fix the problem, but you can email the site owner to let them know.*

Troubleshoot Insecure Connection Errors

- Reload the Page
- Update Your Browser
- Clear Your Browser Cache and Cookies
- Use an SSL Certificate Checker
- Use HTTPS Everywhere
- Check Your Antivirus Software
- Check Your Computer's Date and Time

Note: Make sure you've typed the site's URL correctly. Any small typo could result in the wrong site trying to load, which could lead to a "connection not secure" error.

Recognize Suspicious Links

What to know?

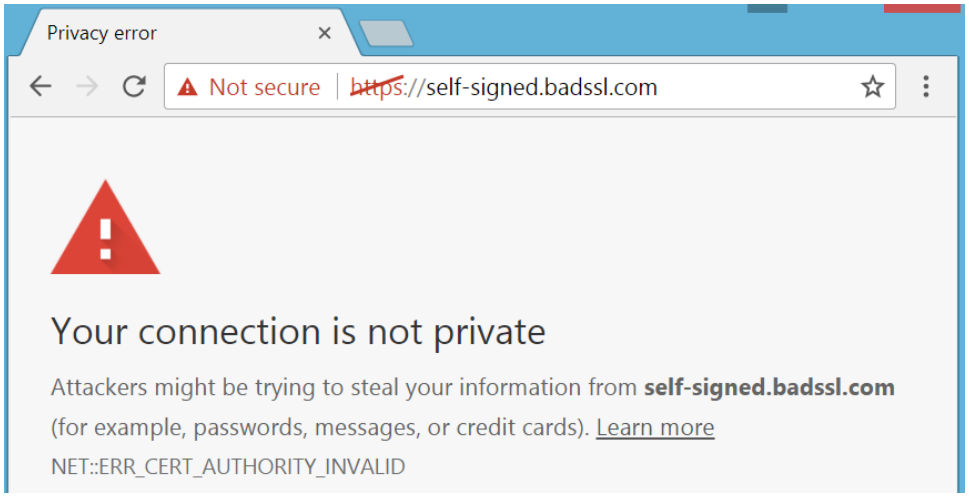
- Inspect short links using a link-expansion service, such as ChecShortURL, or a browser plug-in to show the link's destination.
- Verify solicited emails from your bank or other financial institution by contacting them directly. Don't click any links in the email.
- Decode links with strange character strings with a URL decoding tool, such as URL Decoder, to see the real destination.

What are browser plugins?

A plug-in is a piece of software that manages Internet content that a browser is not designed to process. Graphics in . gif or . jpg-format are usually automatically displayed by the browser. For other file types you may need a special plug-in (also known as add-ons or extensions).

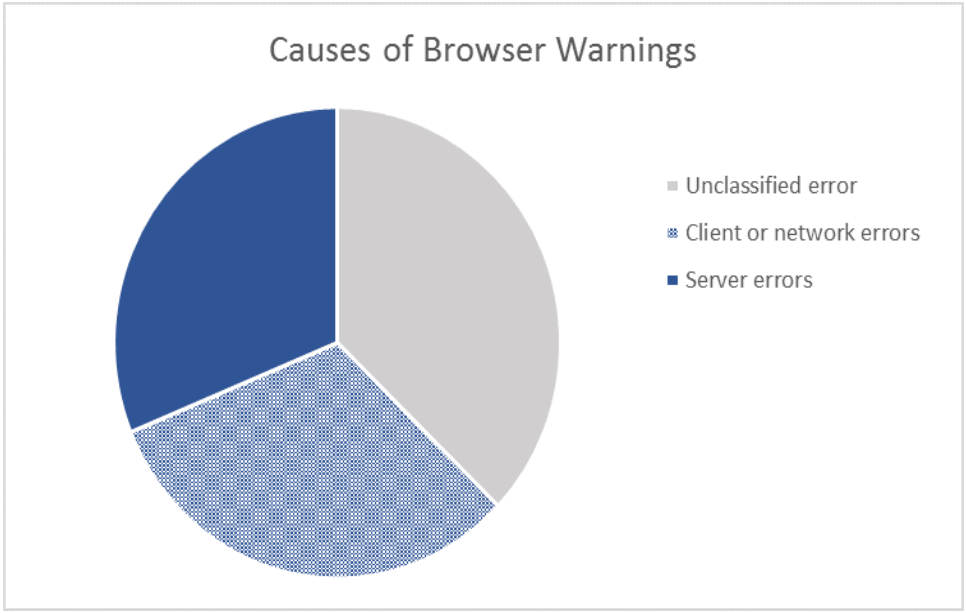
Recognize Untrusted Source Warnings

While these warnings obviously serve a purpose – to prevent users from connecting to sites that are unsafe – many things can trigger these warnings and some of the causes are more serious than others. The concern is that all of these warnings, without a great way for the average user to distinguish the serious ones, not only creates a bad overall user experience, but can lead to users starting to ignore ALL warnings altogether.



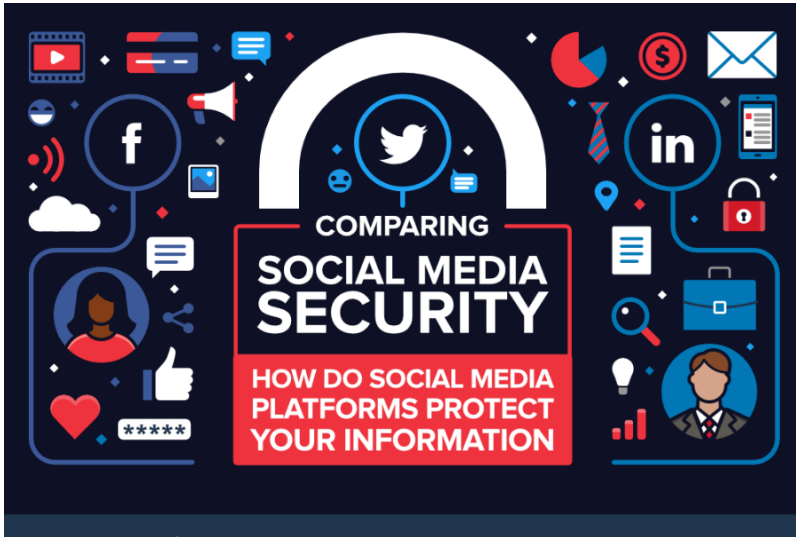
What Are the Most Common Causes of Browser Warnings?

So what's behind these warnings? From a sample of over 300 million errors, collected over approximately one year (see the report for full methodology), Google was able to easily classify the causes of two-thirds of the errors. From there, they categorized the errors into three main types: server, client and network.



Social Media Security

Every industry faces a unique set of risks on social, many of which have put organizations in the press or at the center of controversy. The rise of social media has introduced a new security paradigm, one that puts users—employees, customers and partners—squarely in the attacker's crosshairs. Social media has become the new cyber battleground, presenting one of the largest, most dynamic risks to organizational security in decades.



Simple Steps for Social Media Security

1. Privacy and security settings exist for a reason
2. Once posted, always posted
3. Your online reputation can be a good thing
4. Keep personal info personal
5. Know and manage your friends
6. Be honest if you're uncomfortable
7. Know what action to take